

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |



NASA Policy Directive

NPD 1382.17H

Effective Date: June 24, 2009

Expiration Date: June 24, 2014

COMPLIANCE IS MANDATORY[Printable Format \(PDF\)](#)

Request Notification of Change

(NASA Only)

Subject: NASA Privacy Policy

Responsible Office: Office of the Chief Information Officer

1. POLICY

a. It is NASA policy to protect privacy information that is collected, used, maintained, and disseminated by the Agency. NASA's protections for privacy information shall be compliant with requirements outlined in the Privacy Act of 1974 and amendments, and in other Federal statutes and guidance including the E-Government Act of 2002, the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act and the Office of Management and Budget (OMB) memoranda and circulars. These laws and regulations restrict disclosure of records containing privacy information, grant individuals rights of access and to request an amendment to agency records pertaining to themselves, and require agencies to comply with statutes for the collection, maintenance, and dissemination of records containing privacy information.

b. The NASA collection, maintenance, use, and dissemination of privacy information for both electronic mechanisms and for nonelectronic media shall be in compliance with the Federal statutes and guidance.

c. NASA information and information systems shall use Agency-specific identifiers unless the use of social security numbers (SSN) is mandated by external requirements or is needed to meet the NASA mission or business operation requirements.

2. APPLICABILITY

a. This NASA Policy Directive applies to NASA Headquarters and NASA Centers, including component facilities, and to contractors or other entities that create and/or maintain privacy information for, or on behalf of, NASA as specified in their contract or other governing agreement.

b. For purposes of this directive, privacy information includes:

(1) Information in identifiable form (IIF) is information that directly identifies an individual by name, address, SSN, or other identifying number or code, or other identifying particular assigned to the individual; or a combination of other data elements that could specifically identify an individual when used together, such as gender, race, birth date, and geographic indicators.

(2) Personally identifiable information is information that can be used to distinguish or trace an individual's identity, such as their name, SSN, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

(3) Personal information under the COPPA that is IIF about an individual (from or about a child) collected online, including first and last name; home or other physical address, including street name and name of a city or town; an e-mail address; telephone number; SSN; any other identifier that the Federal Trade Commission determines permits the physical or online contacting of a specific individual; or information concerning the child or the parents of that child that the Web site collects online from the child and combines with an identifier described in this paragraph.

(4) Individually identifiable health information is any information, including demographic information collected from an individual that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

3. AUTHORITY

- a. National Aeronautics and Space Act of 1958 § 203(c)(1), 42 U.S.C. § 2473(c)(1), as amended.
- b. E-Government Act of 2002, Pub. Law No. 107-347, codified at 44 U.S.C. §§ 101 et seq., as amended.
- c. Privacy Act of 1974, 5 U.S.C. § 552a (1988).
- d. Federal Information Security Management Act of 2002, Pub. Law No. 107- 296, codified at 6 U.S.C. Chapter 35, Subchapter III, as amended.
- e. Paperwork Reduction Act of 1995, 44 U.S.C. §§ 3501 et seq., as amended.
- f. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 et seq., as amended.
- g. Health Insurance Portability and Accountability Act of 1976, Public Law No. 104-191.
- h. Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, October 27, 2005.

4. APPLICABLE DOCUMENTS

- a. NASA Privacy Act Regulations, 14 CFR Part 1212.
- b. NPD 2810.1, NASA Information Security Policy.

- c. OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites.
- d. OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.
- e. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
- f. OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy.
- g. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information.
- h. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost of Security In Agency Information Technology Investments.
- i. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

5. RESPONSIBILITY

a. The NASA Administrator shall:

- (1) Designate the NASA Chief Information Officer (CIO) as the Senior Agency Official for Privacy (SAOP).
- (2) Delegate to the SAOP the overall responsibility and accountability for ensuring NASA's implementation of privacy information protections, including the Agency's full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

b. The SAOP shall:

- (1) Have the primary responsibility for the development and implementation of the Agency's privacy policy.
- (2) Carry out the NASA Administrator's responsibilities for privacy.
- (3) Approve Privacy Impact Assessments (PIA).
- (4) Provide OMB with PIAs for planned Information Technology (IT) systems and for collections of information from the public as requested.
- (5) Appoint the NASA Privacy Program Manager.
- (6) Delegate to the NASA Privacy Program Manager oversight, governance, and implementation responsibilities for privacy activities.
- (7) Establish and chair a Data Integrity Board to oversee and coordinate among the various components of the Agency when NASA conducts or participates in a matching program in accordance with the requirements of the Privacy Act.

c. The NASA Privacy Program Manager shall:

- (1) Oversee, manage, and implement the privacy laws, policies, and directives, including the Privacy Act, and other Federal laws and requirements for NASA.

- (2) Ensure compliance with privacy provisions contained in the Privacy Act and other Federal statutes, including the collection, maintenance, use, and dissemination of privacy information.
 - (3) Develop and maintain NASA privacy policies and procedural requirements.
 - (4) Develop Agency guidance for complying with the COPPA.
 - (5) Establish Agency policy, requirements, and process for conducting PIAs for new or revised IT systems and make PIA documentation publicly available, consistent with Federal policy.
 - (6) Provide the Agency's privacy reports required by OMB and the Federal Information Security Management Act (FISMA) to the NASA Senior Agency Information Security Officer and the NASA CIO.
 - (7) Approve Privacy Act Federal Register notices.
- d. The Center Directors and the Director of Headquarters Operations shall:
- (1) Ensure compliance with NASA privacy policies and requirements.
 - (2) Designate a Center Privacy Manager.
- e. The Center CIOs shall:
- (1) Ensure Center adherence to NASA privacy policy and requirements through the respective Center Privacy Manager.
 - (2) Ensure that Information Owners (IOs) and Information System Owners (ISOs) assess the privacy aspects of information and information systems and implement appropriate policies and security safeguards regarding the collection, use, maintenance, and dissemination of privacy information.
- f. The Center Privacy Manager shall:
- (1) Oversee, manage, and implement the privacy policies and requirements, including the Privacy Act, other Federal laws and requirements, and the NASA privacy policy and requirements for their respective Center.
 - (2) Serve as the interface between the NASA Privacy Program Manager and Center personnel on privacy matters.
 - (3) Provide the Center's privacy reports as required by the NASA Privacy Program Manager in support of OMB, FISMA, and Agency requirements.
 - (4) Assist the ISOs and Information Technology Security Managers in conducting PIAs and preparing Privacy Act Federal Register notices.
 - (5) Provide oversight, guidance, and support for investigation and reporting of PII breach incidents.
- g. The Heads of Mission Directorates and Mission Support Offices (MSO) may appoint a Privacy Manager with the same privacy authority, responsibility, and accountability as that of the Center Privacy Managers in accordance with this and other Agency privacy directives.

(1) If a Mission Directorate or MSO Privacy Manager is not appointed, the Center Privacy Manager shall fulfill the privacy responsibilities of the Mission Directorate and MSO activities located at, or under the cognizance of, their Centers.

h. ISOs shall:

(1) Ensure privacy information that is collected from users is properly identified, protected, and controlled in accordance with Federal regulations and NASA policy.

(2) Ensure the secure transmission and storage of privacy information collected by their system(s) in accordance with Federal regulations and NASA policy and procedures.

i. IOs shall:

(1) Ensure privacy information that is collected from users is properly identified, protected, and controlled in accordance with Federal regulations and NASA policy.

(2) Ensure the secure transmission and storage of privacy information collected by contractors or other entities that create and/or maintain privacy information for, or on behalf of, NASA is in accordance with Federal regulations and NASA policy and procedures.

6. DELEGATION OF AUTHORITY

The NASA CIO is delegated authority to carry out the functions and exercise the authority vested in the Administrator to implement, oversee, and manage privacy policy within the Agency pursuant to the authorities cited above.

7. MEASUREMENTS

In assessing whether NASA is in compliance with the current directives or regulations, as applicable, the Agency will accomplish the following:

a. The NASA CIO shall biennially publish a Federal Register Privacy Act notice, as required.

b. The NASA CIO shall provide the Agency privacy report as part of the Annual FISMA report to OMB.

8. CANCELLATION

NPD 1382.17G dated August 24, 2004.

/s/ Christopher J. Scolese
Acting Administrator

ATTACHMENT A: (TEXT)

(URL for Graphic)

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
